

Personal Data Protection Information

IH21 — Digitálny ombudsman, n. o.

I.

Basic Provisions

1. The controller of personal data within the meaning of Article 4(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation; hereinafter the “Regulation” or “GDPR”) is IH21 — Digitálny ombudsman, n. o., ID No. 57273855, Kupeckého 2, 902 01 Pezinok (hereinafter the “Controller”).
2. The Controller’s contact details are: address: Kupeckého 2, 902 01 Pezinok, e-mail: info@digitalniombudsman.cz
3. “Personal data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
4. “Services” means the Controller’s activity consisting in the out-of-court settlement of disputes pursuant to Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).
5. “Other activities” means scientific and research activity aimed at supporting the quality of out-of-court dispute settlement, the organisation of training sessions and conferences aimed at supporting the quality of out-of-court dispute settlement, the popularisation of out-of-court dispute settlement, and the obtaining of financial and other support for the fulfilment of the above objectives.
6. “Marketing” means the sending of newsletters and other information about the Controller’s activities to which you have consented, or the sending of invitations to and registration for events and social occasions organised or co-organised by the Controller, as well as informing you of all related matters and marketing activity connected with the above activities, including the taking of photographic and audiovisual documentation and its further use by the Controller for the purpose of informing about its activities and other marketing activity. The taking and further use of likenesses and of image and sound recordings of natural persons is governed by Sections 11 and 12 of the Slovak Civil Code; general event documentation is taken with prior notice to participants and with the possibility to object, and the Controller will use individual identifiable footage only with the consent of the person depicted.
7. “Other personal data” means communications and documents received by the Controller that cannot be classified in any of the preceding categories.

8. The Controller has not appointed a data protection officer, as it does not meet the conditions under Article 37 GDPR and is therefore not obliged to do so.

II.

Sources and Categories of Personal Data Processed

1. The Controller processes personal data that you have provided to it, or that it has obtained in connection with the provision of the Services under Article I(4), the performance of the Other activities under Article I(5), the handling of the communications and documents referred to in Article I(7), or in connection with the marketing activities under Article I(6).
2. Personal data obtained from other sources: in the course of the Services, the Controller also obtains personal data from the other party to the dispute (in particular from the provider of the online platform), from the parties' representatives or from publicly available sources; this concerns in particular identification and contact data, user identifiers, the content of the disputed material and evidence, and procedural correspondence. The Controller will provide the information required under Article 14 of the Regulation to persons from whom it did not obtain the data directly within one month of obtaining the data at the latest, and in any event no later than at the time of the first communication with them or before the data are first disclosed to another recipient; this does not apply within the scope of the exceptions under Article 14(5) of the Regulation, in particular where the data subject already has the information or where the provision of information proves impossible or would involve a disproportionate effort; in such a case the Controller shall take appropriate measures to protect the data subject's rights, freedoms and legitimate interests, including making this Information publicly available.

III.

Legal Basis and Purpose of Processing

1. The legal basis for the processing of personal data is:
 - the performance of the contract for the provision of the Services between you and the Controller pursuant to Article 6(1)(b) of the Regulation;
 - compliance with the Controller's legal obligations pursuant to Article 6(1)(c) of the Regulation, in particular in the areas of accounting, tax and archiving;
 - the Controller's legitimate interest in the proper, fair and efficient conduct of out-of-court dispute settlement under Article 21 of the Digital Services Act pursuant to Article 6(1)(f) of the Regulation, in relation to persons with whom the Controller has no contractual relationship (in particular the parties' representatives, contact persons of platform providers and third persons referred to in the materials and evidence);
 - the Controller's legitimate interest in protecting the complaint submission system against fraudulent, automated and abusive submissions pursuant to Article 6(1)(f) of the Regulation (see Article V(3) for details);
 - the Controller's legitimate interest in carrying out the Other activities under Article I(5) (science, research, training, popularisation, obtaining support) pursuant to

Article 6(1)(f) of the Regulation; registration for events constitutes performance of a contract pursuant to Article 6(1)(b) of the Regulation;

- the Controller’s legitimate interest in operating the website and handling ordinary communications and enquiries pursuant to Article 6(1)(f) of the Regulation;
- your prior demonstrable consent to receiving the newsletter and commercial communications pursuant to Article 6(1)(a) of the Regulation and Section 116 of Act No. 452/2021 Coll. on Electronic Communications; the Controller sends commercial communications exclusively on the basis of such consent, which you may withdraw at any time, simply and free of charge, in each message or via the Controller’s contact details. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

2. The purpose of the processing of personal data is:

- the provision of the Services under Article I(4), the performance of the Other activities under Article I(5) and the handling of the communications and documents under Article I(7); the provision of services requires personal data necessary for their successful provision (necessary personal data, in particular name and address, contact details – usually e-mail and telephone number, etc.); the provision of personal data is a necessary requirement for the provision of the services, and without the provision of personal data it is not possible to use the services or for the Controller to provide them;
- the sending of commercial communications and other marketing activities specified in Article I(6).

3. The parties to the dispute acknowledge that the information, submissions and evidence they provide to the Controller that are relevant to the assessment of the dispute will, in order to preserve the fairness of the proceedings and the equality of arms, be made available to the other party to the dispute for comment, either by way of access to the digital case file relating to the case in question or by transmission of the relevant materials, in particular by e-mail or via a communication portal designated by the platform; materials cannot be submitted to the Controller on a confidential basis. Personal data that are not necessary for the assessment of the dispute (in particular the complainant’s delivery and contact details beyond their identification) are not disclosed to the other party or are removed or anonymised before disclosure. In the case of exceptionally sensitive content (for example intimate recordings or data capable of seriously interfering with privacy), the Controller, in line with the data minimisation principle under Article 5(1)(c) of the Regulation and the need to protect the rights and freedoms of the persons concerned, limits the further reproduction of such content – in particular, it does not reproduce it in the decision or in further correspondence beyond what is necessary for the assessment of the dispute; the right of both parties to acquaint themselves with the materials at least on an abstract level and to comment on them remains unaffected. When submitting materials and evidence, we recommend limiting personal data concerning yourself and third parties to what is necessary for the assessment of the dispute.

4. Where the materials and evidence submitted in the course of the Services contain special categories of personal data (for example, data revealing political opinions or concerning

health), the Controller processes them on the basis of Article 9(2)(f) of the Regulation, i.e. to the extent necessary for the establishment, exercise or defence of legal claims in the course of the out-of-court settlement of the dispute.

5. Where the materials contain personal data relating to criminal convictions and offences or related security measures within the meaning of Article 10 of the Regulation, the Controller further processes them in identifiable form only where such processing is specifically authorised by Union or Slovak law providing for appropriate safeguards for the rights of the data subject; otherwise it removes or anonymises them before any further use.
6. The Controller does not carry out automated individual decision-making or profiling within the meaning of Article 22 of the Regulation.

IV.

Data Retention Period

1. The Controller retains personal data:
 - for the period necessary for the conduct of the proceedings and subsequently for the establishment, exercise or defence of specific legal claims; the length of subsequent retention is determined by the limitation period of the law governing the specific claim, with the period of 15 years constituting an absolute ceiling applied only where legislation providing for such an objective limitation period demonstrably applies to the specific claim; otherwise the shorter relevant period applies. Once the ground ceases to exist, the data are erased or anonymised unless a separate legal basis for their further processing exists;
 - documents required by accounting and tax legislation for the period laid down by such legislation (as a rule 10 years);
 - contact details for the newsletter until consent is withdrawn; the Controller retains proof of the granting and withdrawal of consent for at least four years from its withdrawal (Section 116 of Act No. 452/2021 Coll.).
2. Upon expiry of the retention period, the Controller shall erase the personal data unless they are subject to mandatory archiving.
3. The Controller shall also erase personal data and all other documents obtained in connection with the Services where the purpose of their processing ceases to exist (storage limitation pursuant to Article 5(1)(e) of the Regulation), in particular where it concludes that it no longer needs them for the provision of the services, including the contents of the case file and documents received from the parties to the dispute or their representatives. However, personal data and other documents shall not be erased under this paragraph before a decision terminating the out-of-court dispute settlement process has been issued.
4. After the original purpose has ceased, the Controller may further process selected data for scientific or historical research purposes or for statistical purposes only where such further processing is permissible under the Regulation and a legal basis for it exists. Anonymised data are used preferentially. Where the purpose cannot be achieved without identifying individuals, appropriate safeguards pursuant to Article 89(1) of the Regulation shall apply,

in particular pseudonymisation and data minimisation. Following the lapse of the original purpose, special categories of personal data are used exclusively in anonymised form, unless a separate legal basis under Article 9(2) of the Regulation applies.

V.

Recipients of Personal Data (the Controller's Subcontractors)

1. The recipients of personal data are persons:
 - involved in the delivery of services or the execution of payments under a contract,
 - involved in ensuring the operation of the services,
 - providing marketing services.
2. Personal data are processed on the Controller's behalf in particular by the following processors: Google (Google Workspace – e-mail communication and management of the digital case file; data at rest stored in the Europe data region), Jotform Ltd (operation of the online complaint form; data stored on servers in the EU – Frankfurt am Main) and Cloudflare, Inc. (security and operation of the Controller's website), each on the basis of a contract pursuant to Article 28 of the Regulation, and further by a provider of a specialised IP address assessment service (verification of submissions – see paragraph 3).
3. For the purpose of protecting the complaint submission system against fraudulent and automated submissions (the Controller's legitimate interest pursuant to Article 6(1)(f) of the Regulation), the IP address from which a complaint is submitted may be transmitted to a specialised external IP address assessment service for an assessment of whether it shows the characteristics of an anonymising service (VPN, proxy, datacenter). The result of the assessment serves solely as an input for human review of the submission; no decision-making based solely on automated processing within the meaning of Article 22 of the Regulation takes place. You have the right to object to this processing at any time pursuant to Article 21 of the Regulation.
4. The Controller may transfer personal data to a third country (a country outside the EU/EEA), in particular in connection with the use of the cloud, mailing or similar services referred to in paragraph 2. Any such transfer is safeguarded in accordance with Chapter V of the Regulation: in the case of Google and Cloudflare, by certification under the EU–U.S. Data Privacy Framework, supplemented by standard contractual clauses pursuant to Article 46(2)(c) of the Regulation; in the case of Jotform, by the storage of data in the EU and by the certification of Jotform Inc. under the EU–U.S. Data Privacy Framework for exceptional cases of disclosure; and in the case of the IP address assessment service, by ensuring that the processing takes place exclusively in the EU/EEA or in countries covered by a European Commission adequacy decision, or is covered by standard contractual clauses pursuant to Article 46(2)(c) of the Regulation. A copy of the applicable safeguards for transfers of personal data to a third country, or information on where those safeguards are available, may be obtained upon request at info@digitalniombudsman.cz.

VI.

Your Rights under the Regulation

1. Under the conditions laid down in the Regulation, you have:
 - the right of access to your personal data pursuant to Article 15 of the Regulation;
 - the right to rectification of personal data pursuant to Article 16 of the Regulation, or restriction of processing pursuant to Article 18 of the Regulation;
 - the right to erasure of personal data pursuant to Article 17 of the Regulation;
 - the right to object to processing pursuant to Article 21 of the Regulation;
 - the right to data portability pursuant to Article 20 of the Regulation;
 - the right to withdraw consent to processing in writing or electronically to the address or e-mail of the Controller specified in Article I of these terms.
2. You also have the right to lodge a complaint with the competent supervisory authority, which is in particular the Office for Personal Data Protection of the Slovak Republic (Úrad na ochranu osobných údajov Slovenskej republiky, www.dataprotection.gov.sk); pursuant to Article 77 of the Regulation, you may also lodge a complaint with the supervisory authority in the Member State of your habitual residence or place of work, if you believe that your right to the protection of personal data has been infringed.

VII.

Personal Data Security Conditions

1. The Controller declares that it has adopted all appropriate technical and organisational measures to secure personal data.
2. The Controller has adopted technical measures to secure data storage facilities and storage of personal data in paper form, in particular regular software updates, the use of antivirus programmes, the use of trustworthy storage facilities and providers of the software used, and appropriate technical security of the Controller's registered office.
3. The Controller declares that only persons authorised by it have access to personal data.

VIII.

Cookies and Similar Technologies

1. The Controller's website uses exclusively technically necessary cookies and similar technologies, without which the website cannot be operated securely and a complaint cannot be submitted. In accordance with the applicable electronic communications legislation (in the Slovak Republic, Section 109(8) of Act No. 452/2021 Coll. on Electronic Communications), no consent is required for these cookies.
2. Technically necessary cookies serve in particular to: secure and protect the website against automated and malicious traffic (currently the Cloudflare service), operate the complaint form (currently the Jotform service), distinguish human from automated submissions (currently the hCaptcha service), and store your cookie choice (the cookie banner, currently the CookieScript service). A detailed and up-to-date overview of the individual

cookies, including their validity periods, is available at any time in the cookie settings on the website.

3. Analytics cookies used to measure website traffic (the number and source of visits and the approximate geographic area; currently the Google Analytics service) are used by the Controller exclusively on the basis of your consent given via the cookie banner. You may withdraw or change your consent at any time in the cookie settings on the website, without affecting the lawfulness of prior processing. Where the provider of the analytics tool processes data in the United States, the transfer is safeguarded by its certification under the EU–U.S. Data Privacy Framework or by standard contractual clauses pursuant to Article 46(2)(c) of the Regulation. The Controller does not use marketing cookies.
4. You may delete or block cookies at any time in your browser settings; however, blocking necessary cookies may prevent the submission of a complaint. Should the Controller introduce further categories of cookies in the future, they will be deployed only after consent has been obtained, and this information will be updated accordingly.

IX.

Final Provisions

1. You will be acquainted with this Personal Data Protection Information at the time your personal data are obtained, in particular by means of a link made available directly in the complaint form before its submission. The current version of the Personal Data Protection Information is always available on the Controller's website.
2. The Controller is entitled to amend these terms at any time. The Controller will publish the new version of the personal data protection terms on its website and will inform you of the change in an appropriate manner.

This information takes effect on 1 September 2026 and replaces the version effective from 29 May 2026.